UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

---X

UNITED STATES OF AMERICA,

-v-

JOSHUA ADAM SCHULTE,

Defendant.

17 Cr. 548 (PAC)

OPINION & ORDER

---X

This Order resolves the Rule 29 motion brought by Defendant Joshua Schulte ("Schulte"), a former Central Intelligence Agency ("CIA") employee, charged with stealing national defense information and transmitting it to Wikileaks. On March 9, 2020, after a four-week trial, a jury returned a partial verdict convicting Schulte of two counts: making false statements to law enforcement (Count Eight) and contempt of court (Count Ten). The jury failed to reach a verdict on the remaining eight counts, and, as a result, the Court granted a mistral as to those counts.[1] Schulte moves for a judgment of acquittal as to all counts, including those for which the jury did not reach a verdict. *See* Def. Mot., ECF No. 397. The Government has filed its opposition at ECF No. 410.

After careful consideration and thorough review of the record, the Court denies Schulte's Rule 29 motion, except as it pertains to a limited portion of the Government's case concerning Count Three.[2]

[1] Schulte has subsequently been reindicted, and now faces a second trial whose date has yet to be set. *See* ECF No. 517. Judge Furman will preside over the second trial. *See United States v. Schulte*, 17-CR-548 (JMF), Notice of Case Reassignment (S.D.N.Y. Oct. 18, 2021).

[2] During trial, the Government belatedly revealed to defense counsel that the CIA had placed one of the

BACKGROUND[3]

I. The Government's Case

A. Motive: Schulte's Problems at the CIA

In the fall of 2015, Schulte's ongoing feud with a CIA colleague, Amol, began to escalate. On October 2015, Schulte and Amol both complained to their supervisor about each other. GX 1019; GX 1020.[4] Specifically, Schulte reported that Amol made "derogatory and abusive comments" to Schulte and his colleagues including: "'I wish you were dead,' 'I wish you'd die in a fiery crash and burn, oh I would be so happy.'" GX 1038; Weber Tr. 277. One CIA employee, Weber, testified that although he never heard Amol make derogatory or abusive comments to others, he did witness Amol saying things like this to Schulte. Weber Tr. 277–78. There was general consensus among CIA witnesses that the two men did not get along.

In February 2016, Amol and Schulte had a heated exchange at work. Weber Tr. 271–73. Shortly thereafter, Schulte emailed the CIA's security office ("Security") to complain that Amol had been abusive and made death threats towards him. GX 1038. Schulte reported that on March 1, 2016, after being "unusually quiet" that morning, Amol had suddenly appeared "directly behind [Schulte], unusually close, towering over [Schulte]," and threatened Schulte's life, causing Schulte to be "frightened and very concerned." GX 1038; Weber Tr. 279–80. CIA witnesses characterized

Government's witnesses, Michael, on enforced administrative leave. Although the CIA sanctioned Michael in August 2019 the Government failed to inform defense counsel of Michael's enforced administrative leave until February 11, 2020, the day before Michael's direct examination. Schulte filed a motion for a mistrial based on the Government failure to disclose Brady evidence. *See* Brady Mot., ECF No. 328. Schulte later conceded that his motion had been mooted by the resolution of his first trial (*see* ECF No. 428 at n. 1), and the Court has since formally denied it as such. *See* ECF No. 514. The Court, however, notes *infra* for the record the steps taken in light of the Government's eleventh-hour disclosure.

[3] The following description of the evidence at trial is relayed in the light most favorable to the Government. *See United States v. Glenn*, 312 F.3d 58, 63 (2d Cir. 2002). The Court draws all reasonable inferences in the Government's favor. *See id.*

[4] Citations so the trial transcript are denoted as "Tr.", while citations to Government and Defense Exhibits are denoted, respectively, as "GX" and "DX."

Schulte's claims about Amol as "exaggerated" and "out of context"; they testified that they did not believe Schulte's claims and that they had not witnessed Amol threaten others. Stedman Tr. 1502–03; Weber Tr. 277–81; Sean Tr. 1633–35.

Shortly after the incident, Schulte filed a motion for a protective order against Amol in state court, which was initially granted. Weber Tr. 282–84; GX 1619. Following the protective order, management reassigned both Schulte and Amol to two different branches within the Engineering Development Group ("EDG"), the group for which both men worked. Weber Tr. 283. On March 29, 2016, Schulte received an email directing him to move to a new cubicle. GX 1046. He replied: "I just want to confirm that this punishment of removal from my current branch is for reporting to security an incident in which my life was threatened and/or for submitting a protective order against [Amol]." *Id.* Schulte also filed an Outside Activity Request, as per CIA policy, indicating that he intended to meet with an attorney to pursue legal action and suggesting that the media might become involved. GX 506; Small Tr. 2007.

During trial, the jury listened to a recorded interview of Schulte conducted by Security on April 6, 2016. GX 508. During that interview, Schulte expressed, among other things, that he felt he was being unfairly punished for reporting Amol's conduct; that "no one seems to have [his] back"; and that he would do whatever he had to do "to make the situation right" and to "shed light on this" including going to the media *Id.* When asked what result he was hoping for, Schulte answered he would like to "sit down with his management"—that he felt there needed to be "some kind of punishment" for them, including "some kind of apology" or "some kind of acknowledgement they made a mistake." *Id.*

The Reassignment. Schulte's reassignment entailed more than a desk move. As a developer in the CIA's Center for Cyber Intelligence, Operations Support Branch ("OSB") Schulte worked on developing cyber tools for the CIA. The move to his new branch implicated his access to programs, projects, and tools that he had previously worked on, including two tools in particular: OSB Libraries and Brutal Kangaroo.

Following his move from OSB, Schulte's colleague (not supervisor) Weber revoked Schulte's administrative privileges to OSB Libraries, which was a collaborative database of code accessible by all branches within Schulte's group, including the branch Schulte had been reassigned to. Weber Tr. 287–88; Michael Tr. 1207. Days later, on April 14, 2016, Schulte confronted Weber about revoking Schulte's administrative privileges to OSB Libraries without telling him. GX 1062; Weber Tr. 289–90. Weber explained that he had done so because Schulte had been reassigned. *Id.* When Schulte took issue with this rationale, Weber suggested Schulte discuss the matter with their supervisor, Sean. *Id.* Schulte then spoke with Sean about OSB Libraries, but, according to Sean, the issue of administrative privileges was not explicitly addressed. Sean Tr. 1651–52, 1659. It was clear from the record, however, that Schulte's reassignment would not have implicated his *read*-access to contribute to or pull from OSB Libraries; Schulte would thus have needed Sean's approval only to restore his now-revoked *administrative* privileges. *Id.*; GX 1062.

After meeting with Sean, Schulte reported to Weber that Sean had signed off on reinstating Schulte's administrative privileges for OSB Libraries. Weber Tr. 290. Weber responded that he would discuss the issue with Sean, prompting Schulte to reply that Weber should restore Schulte's privileges now because the reinstatement was "going to happen one way or another." *Id.* Later, Weber emailed Schulte, copying management, to inform him that he had followed up with Sean, and that he would not restore Schulte's administrative privileges. GX 1061. Schulte replied: "Hey guys, thanks for the email. . . . Since the OSB libraries were initially my idea that stemmed from

Brutal Kangaroo, and I've spent a lot of time and effort managing and helping administer them, I'd like to stay on along with [Frank Stedman] and [Jeremy Weber] as helping administer them. . . . So if OSB and RDB would be okay with this, I would like to continue my active role with the libraries." *Id.*

After receiving this email, Weber checked the OSB Library audit logs. Weber Tr. 297. Upon observing that Schulte had in fact already reinstated his own administrative privileges on OSB Libraries, he immediately reported this issue to his management, who in turn flagged it to Security. GX 1062; Weber Tr. 528. Weber's report caused concern at the CIA because Schulte's self-granting of access was not in accordance with CIA policy and called into question whether Schulte could be trusted with classified information. Leonis Tr. 577–601. None of the CIA witnesses, however, could identify a written policy or standard operating procedure that required removal of Schulte's administrative privileges on projects following a branch move. *See* Weber Tr. 437; Leonis Tr. 684.

B. Means: Incomplete Revocation of Schulte's Administrative Privileges

Schulte restored his access to OSB Libraries using his administrative privileges to the Atlassian services on the DEVLAN system. GX 1062. In response, management directed Weber and two system administrators, David and Tim, to remove all developers' (including Schulte's) administrative privileges to Atlassian services on DEVLAN. David Tr. 792–804. The Atlassian services on DEVLAN were a commercially available suit of software used by the CIA to store classified information. Weber Tr. 215–18. The Atlassian services included programs such as Confluence (EDG's Wikipedia-like page in which users could comment on the group's work) and Stash (the repository for, among other things, source code for cyber tools), among others. *Id.* at 174, 215–18.

On Saturday April 16, 2016, David and Tim began eliminating Schulte and the other developers' administrative privileges. David Tr. 792–804. Before making any system changes, however, they first created a "snapshot" of the Confluence database (the "April 16 Snapshot"). *Id.*; *see also* GX 1207-92; GX 1703 at 51–66. The April 16 Snapshot was a frozen-in-time copy of the Confluence database as it existed on April 16; armed with this safeguard, if any of their changes yielded unintended side effects, David and Tim could simply restore the system to its April 16 state. David Tr. 792–804.

As a result of the April 16 changes, Schulte was no longer allowed administrator access to Atlassian programs, and therefore was no longer allowed direct access to the Atlassian backup files (the "Alta Backup Files," some of which would be published by Wikileaks less than a year later). David Tr. 792–804. These backup files were created by the Atlassian products, including Confluence and Stash, and saved daily to the "Altabackup" folder. *Id.* at 788. Prior to April 16, Schulte and a few others had access to DEVLAN and the Alta Backup Files. Weber Tr. 215–18. Schulte's administrative privileges on DEVLAN had allowed him to, among other things, manage the Atlassian services and grant access to those who needed access to certain services; Schulte maintained administrator access and managed the system for a significant period prior to April 16, 2016. *Id.* at 213. Schulte, unlike regular DEVLAN users, was intimately familiar with the Alta Backup Files because he wrote the computer code that was used to create them, was involved in making Alta Backup Files accessible to administrators, and managed the Alta Backup Files including, for example, deleting old files when they took up too much space. *Id.* at 223–26, 238, 252–57.

The April 16 system changes revoked these privileges. However, unbeknownst to Dave and Tim, Schulte still had access to an "SSH Key" for the OSB ESXi server, which in effect allowed him continued backdoor access to parts of DEVLAN with administrative privileges. Leedom Tr. 1030.

On April 18, 2016, Schulte returned to work to find that his administrative privileges to DEVLAN had been revoked over the weekend without his knowledge. GX 1063. That morning, he met with his division supervisor, Anthony Leonis, who reprimanded him for restoring his own access to OSB Libraries and presented him with a memorandum articulating the prohibition on self-granting access to administrative privileges, which Schulte signed. GX 1095. That same day, Schulte attempted to access various parts of DEVLAN as an administrator. Leedom Tr. 1019, 1022–23, 1032. He managed to log into the OSB ESXi Server as an administrator because his SSH key still worked. *Id.* at 1029–30, 1032. Nonetheless, at approximately 1:00 p.m. that day, Schulte reported to Leonis that he had "verified that all private keys with access have been destroyed/revoked without notice" and that "[i]t seemed like overnight (literally) all my permissions within the products were removed and all my permissions on the servers themselves revoked. And all without anyone informing me." GX 1063. At the time Schulte sent this email, he was logged into the OSB ESXi server as an administrator, aware that he still had some administrative access despite his email attesting otherwise. Leedom Tr. 1032–33, 1048.

Expert testimony established that on the evening of April 18, 2016, Schulte reviewed log files on the OSB server documenting information about every computer command that was entered into the system, such as the date and time of the command, and all login attempts to the server. Leedom Tr. 1038–48; GX 1209-13; GX 1203-43; GX 1209-44; GX 1209-8. Reviewing those files enabled Schulte to see what activity the system was recording. *Id.* Schulte locked the vault on his floor that night, indicating that he was last person physically present in the vault when he accessed the log files. GX 105.

C. Opportunity: Schulte's April 20 Access to DEVLAN and the Alta Backup Files

Forensic Evidence. To prove Schulte accessed the leaked files, the Government presented evidence showing that: (1) Schulte reverted the compromised system (DEVLAN) to a state where he had full administrative privileges and thus access to the stolen files; (2) the stolen Confluence Alta Backup File date-accessed timestamp was modified during the reversion; (3) the system was reverted for a long enough time to copy the stolen files; (4) Schulte deleted log files that would have shown his activity on the system, as well as the April 20, 2016 snapshot that he used to restore the system back to the present day; and (5) that Schulte was, in fact, at his DEVLAN computer during the reversion. The Government did not offer any evidence that specifically pertained to the stolen Stash Alta Backup File though, like the stolen Confluence Alta Backup File, it would have been accessible to Schulte during the reversion. And the Government offered no evidence of any device used to store or transport the stolen files from DEVLAN, an air-gapped network (i.e. a network that is not connected to the internet), and out of the building.

On April 20, 2016 at 5:29 p.m., Schulte used the administrative account on the OSB server to create a snapshot of Confluence titled "bkup." Leedom Tr. 1060–62; GX 1202-17; GX 1209-7. At 5:35 p.m., Schulte reverted Confluence to the April 16, 2016 snapshot. Leedom Tr. 1063–64; GX 1202-18. The reversion reinstated Schulte's since-revoked Atlassian administrative privileges on DEVLAN, allowing him to access the Alta Backup Files. Leedom Tr. 1049. The Government elicited testimony that such reversions to an old snapshot were far from commonplace, and would typically be appropriate only where something catastrophic had befallen a system. David Tr. 829.

The March 3, 2016 Confluence Alta Backup File—later leaked to Wikileaks—was accessed in the Alta Backups folder at 5:43 pm on April 20, 2016. Leedom Tr. 1050. The Government's expert drew this conclusion from the "date accessed" timestamp attached to the March 3, 2016 Confluence Alta Backup File. *Id.* This timestamp—which changes when, among other actions, the file is copied—identified the file as last having been accessed during the Confluence reversion. *Id.* The forensic evidence also showed that, unlike the March 3 Confluence Alta Backup File, the other Confluence Alta Backup Files from the weeks surrounding March 3 displayed date-accessed timestamps matching the date and time each backup file had originally been created. GX 1207-27.

The system stayed in the reverted state for over an hour until 6:51 p.m.—enough time to copy the Confluence and Stash backups. Leedom Tr. 1049–50; GX 1255. At that point, using the April 20, 2016 "bkup" file he had just created 82 minutes earlier, Schulte restored Confluence back to the April 20, 2016 state it had been in prior to the reversion. Leedom Tr. 1063. Finally, at 6:55 p.m., he deleted the records (i.e., log files) of his conduct, as well as the "bkup" file he had just used to restore the system back to its present-day state. *Id.* at 1063–66. The effect of deleting the log files and "bkup" snapshot was to erase any trace of Schulte's actions on the server since 5:29pm. *Id.* The log files would have recorded, for example, a command to copy the stolen data. *Id.* Schulte did not, however, delete the log files from his own workstation. *Id.* at 1066–67.

Undisputed expert testimony demonstrated Wikileaks disclosures included data from the March 3, 2016 Confluence Alta Backup File, as well as Stash data from a similar timeframe. Berger Tr. 1363–1366.

Documentary Evidence. In addition to this forensic evidence, the jury was presented with documentary evidence establishing Schulte's presence at his DEVLAN computer at the time of the theft. This included: (1) an email Schulte sent to Leonis during the reversion, minutes after the Alta Backup Files were accessed (GX 1070); (2) Sametime chat logs with another employee, Michael, from minutes after the Alta Backup Files were accessed (GX 719; Michael Tr. 1208–09); (3) Schulte's DEVLAN chat logs with Michael about going to the gym, timestamped shortly before the reversion ended (GX 1202-25; Michael Tr. 1215–16); and (4) badge records showing that Schulte locked the 8th floor vault on the evening of April 20, suggesting that he was the only person on the floor when the reversion concluded (GX 105; Leedom Tr. 1100). In fact, the only two times Schulte locked the 8th floor vault in 2016 were on April 18, when he viewed administrative log files on the OSB ESXi server after being told he was no longer an administrator, and April 20, the night of the theft. GX 105.

The jury also heard substantial testimony concerning the lackluster security of the DEVLAN system itself. *See* GX 5001. The CIA protected DEVLAN by restricting outside access to it; sequestering it from the internet; limiting access to approximately 200 individuals, each of whom possessed a Top Secret security clearance; requiring badges to enter the locked rooms secured by vault doors in which DEVLAN terminals were stored; and protecting the CIA building in which the system was housed with armed guards and perimeter fencing. *See* Tr. 187, 194–96, 213, 552, 779, 900–01, 907. Nonetheless, DEVLAN was described by many CIA employees as the "wild wild west"—it was open, collaborative, flexible, and lacked the sort of use policies found on other CIA networks; it hosted malware that the CIA designed and tested to infect other systems in foreign countries; it was a "dirty network," meaning it contained information not solely created by the owners of that network; it was accessible to users in two foreign offices; it lacked controls and security monitoring tools; and its users employed shared passwords. *See* Tr. 416–23, 839–43, 1238–41; GX 5001. The system had also experienced security snafus including, for example, an incident where an employee using a laptop connected to wi-fi had plugged into the DEVLAN system for four hours before being detected. David Tr. 846. And according to the Government's own theory of the case, no one at the CIA realized information had been stolen from DEVLAN until it appeared on Wikileaks, nearly a year later. *See* Weber Tr. 351.

D. Transmission: Schulte's Actions Following the Reversion

To prove transmission, the Government offered circumstantial evidence from the weeks immediately following the theft, including: (1) Schulte's April 20, 2016 reversion corresponding with the time during which the Alta Backup File was accessed; (2) Schulte downloading, on his home computer, programs facilitating the anonymous and secure transfer of data, including programs recommended by Wikileaks; (3) Schulte's purchase of external hard drives for same-day delivery; (4) Schulte's Google searches regarding "wiping" or deleting data, "hashing" (a technique used when transferring data), and the transfer of 1TB of data; (5) Schulte's actions on his computer during and throughout the middle of the night on April 30 to May 1, 2016; (6) Schulte's complete reformatting of his computer on May 5, 2016, which had the effect of erasing data; and finally (7) Schulte's increased interest in Wikileaks in the summer and fall of 2016. The Government, however, did not present any direct evidence that Schulte brought devices home from the CIA or any direct evidence that Schulte took data from the CIA and put it on his home computer. Berger Tr. 1427–28. The Government's expert testified that, in the course of the investigation, authorities did not recover any direct evidence of stolen Alta Backup Files on Schulte's home computer. *Id.*

The day following the reversion, April 21, 2016, Schulte emailed his boss, Leonis, about transferring the OSB Server equipment out of his name and modifying his access—the same server and access used to log into DEVLAN the night before. GX 1071. Schulte also erased the logs and contents of a USB drive he had used the day before on his DEVLAN workstation prior to the reversion. GX 1205-1.

The next link in the Government's chain of circumstantial evidence centered around Schulte's actions at home. On April 23, 2016, he added to the Eraser Portable (a secure deletion software) queue for deletion a folder entitled "Brutal Kangaroo," the name of a cyber tool he had developed at the CIA. GX 1404-6; Berger Tr. 1389. Schulte also added to the Eraser Portable queue five encrypted files he stored at home on his "D drive," but did not delete them. GX 1404-6; Berger Tr. 1372–75, 1389–93. On April 24, 2016, Schulte ordered for same-day delivery external hard drives. Berger Tr. 1375–77. That same day, he downloaded Tails, a program that facilitates the anonymous transfer of information over the internet, and a Wikileaks-recommended mechanism for transmitting information in conjunction with the program TOR, which was also installed on Schulte's home computer. *Id.* at 1381–33.

On April 30 at 11:28 a.m., Schulte downloaded Darik's Boot and Nuke—a commercially available program that securely deletes data. GX 1402-10; Berger Tr. 1393–96. Later that night shortly before 11:00 p.m., Schulte searched on several occasions for secure wiping utilities and visited related websites, including a website entitled "Kill Your Data Dead With These Tips and Tools." GX 1305-9; Berger Tr. 1408–09. At 12:19 a.m. on May 1, 2016, Schulte mounted the D drive, where certain encrypted files were located, onto his home computer's virtual machine. GX 1401-1. Over the next several hours, he repeatedly unlocked his computer at 1:57 a.m., 2:34 a.m., and 2:56 a.m. GX 1401-1. At approximately 3:18 a.m. on May 1, Schulte searched several times for information about "hashing" large files (a technique to confirm the integrity of transferred data) and visited websites entitled "What Is the Fastest Way to Hash MD5 Large Files" and "How Can I Verify that a 1TB File Transferred Correctly." GX 1305-9; Berger Tr. 1404.

On May 5, 2016, Schulte reformatted his home computer, including the D drive that contained the encrypted files. Berger Tr. 1407–08. Schulte's reformatting had the effect of erasing the drives so that any data stored prior to the May 5, 2016 reformat would have been overwritten. *Id.*

E. Aftermath: Schulte's Resignation from the CIA and Interest in Wikileaks

According to the Government's expert, due to the format of the Alta Backup Files it would have taken Wikileaks a significant time to prepare it for public dissemination. Leedom Tr. 1113–33. Schulte continued working for the CIA for over six months following the reversion. GX 1616.

In August 2016, Schulte began searching the internet regularly for information regarding Wikileaks. Between August 2016 and January 2017, he conducted at least 39 Google searches for Wikileaks and related terms and visited 1115 related webpages. GX 1352. Significantly, prior to August 2016 Schulte had conducted just three searches for Wikileaks and visited nine related webpages. GX 1351. The Government's expert witnesses acknowledged, however, that during the same time period—the summer and fall of 2016—Wikileaks prominently published information related to the 2016 national election, which garnered substantial attention. Rosenzweig Tr. 54–55; Evanchec Tr. 2272. Schulte also searched for Wikileaks code, which the Government's witnesses testified was significant because at that point, Wikileaks had never published source code; the Alta Backup Files, however, contained source code, which was eventually disclosed by Wikileaks. Rosenzweig Tr. 74–75. On January 4, 2017, Schulte search for "Wikileaks 2017" and visited a webpage entitled "Wikileaks Vows to 'Blow You Away' in 2017 'Showdown.'" GX 1352.

On November 10, 2016, Schulte's last day at the CIA, Schulte sent an email to the CIA's Office of Inspector General ("OIG"). GX 1119. In the email, Schulte wrote that he was resigning because he had expressed concerns about DEVLAN's security to his supervisors, but the concerns had gone unaddressed and management had retaliated against him for contacting security. *Id.* Schulte added that he was forced to manage the Atlassian services despite no official job title or training because the contractors hired to manage the system were incompetent. *Id.* In his view, this "left [DEVLAN] open and easy for anyone to gain access and delete our entire EDG source code repository or even easily download and upload it in its entirety to the internet . . . . Luckily, nothing happened but it still illustrates the lack-of-security and pure ineptitude of [one of Schulte's superiors] Karen." *Id.* Government witnesses, including Karen, testified that Schulte had never reported security concerns to his management chain and was not targeted by management for raising purported complaints about DEVLAN security. Evanchec Tr. 2206; Karen Tr. 1721. After Schulte resigned, he moved to New York City and took a job at Bloomberg. Schlessinger Tr. 2475.

F. The Leaks

On March 7, 2017, Wikileaks posted the first of the leaks online, dubbed the "Vault 7 and 8 Leaks." The first leak contained information from the Confluence March 3, 2016 Alta Backup Files, the same file with a modified date-accessed timestamp during the reversion on April 20, 2016. GX 1; Leedom Tr. 1113–33; Berger Tr. 1350–66. In subsequent releases, Wikileaks posted data about several tools from Stash, including source code. Weber Tr. 174.

Within a week of the first leak, the FBI identified Schulte as a suspect and mounted a full-court press: Schulte was placed under 24/7 surveillance; agents covertly searched his apartment; the FBI issued subpoenas to Google, Twitter, Facebook, Reddit, Apple, and Microsoft; the FBI also put a pen register on Schulte's devices; and it used undercover employees and confidential human sources, including his former CIA co-workers, in its investigative efforts. *See* Evanchec Tr. 2280–94; 2346–58.

The FBI also interviewed Schulte several times; Schulte cooperated voluntarily. Evanchec Tr. 2338. The jury heard evidence that during these interviews Schulte (1) denied having a copy of the classified email to the OIG (even though the FBI recovered a copy of the email in his apartment in New York City) (GX 1616); (2) denied taking information from DEVLAN home (despite old chats with friends indicating that he took information from DEVLAN to his home) and (3) denied making DEVLAN vulnerable to theft (despite deleting log files on April 20, 2016). Although the FBI repeatedly asked Schulte about his DEVLAN activities, he never mentioned anything related to his activities on April 20, 2016. *Id.* at 2178. Nor did he confess that he was responsible for the leaks. *See id.* at 2349–50, 2355.

G. Schulte's Indictment and Conduct in Prison

To prove contempt, the Government introduced evidence that Schulte violated the Court's Protective Order, including that he emailed a reporter a copy of the search warrant affidavit, as proscribed under the Protective Order. GX 812. To show Schulte disclosed classified information while incarcerated at the Metropolitan Correctional Center ("MCC"), the Government presented evidence that, while at MCC, Schulte drafted tweets about a classified CIA cyber tool, Bartender (GX 809) and attempted to publish an article entitled "Malware of the Mind" containing information about CIA tradecraft on his blog called "Presumption of Innocence" (GX 801, 809). CIA witnesses testified that these materials contained classified information that had never been publicly disclosed, and that disclosure could cause significant harm to CIA operations and personnel. *See* Stedman 1514–15; Michael Tr. 1218–19.

In May 2018, news articles were published about the Schulte case, including one authored by a reporter at the Washington Post. Schlesinger Tr. 2467–68. The Court held a conference on May 21, 2018 at which it reiterated to Schulte the terms of the Protective Order, including that

Schulte was not permitted to provide documents subject to the Protective Order to third parties, like reporters. GX 829. The Court also instructed Schulte, "If you want to vary the terms of the protective order, your relief is not to do it on your own, Mr. Schulte, but to have your lawyer come into court and explain why there should be a modification of the order." *Id.* at 7. Schulte confirmed that he "now" understood the Court's instructions and the terms of the Protective Order. *Id.* at 8.

In July 2018, Schulte became increasingly frustrated about his case as well as his family's failure to post publicly his articles, including "Malware of the Mind." GX 801, 809. He wrote in his notebook in July 2018: "Ugh talked to my parents today & found out that my fucking articles that were uploaded to [Facebook] . . . were the wrong fucking articles." GX 806. In an entry dated August 8, 2018, he wrote: "If gov't doesn't pay me $50 billion in restitution & prosecute the criminals who lied to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery that is the USG. I will look to break up diplomatic relationships, close embassies, end U.S. occupation across the world." GX 809. The jury heard testimony that Schulte was capable of releasing damaging information because of the sensitive nature of his work at the CIA. Schlesinger Tr. 2649–52.

On August 13, 2018, Schulte obtained a contraband cellphone in prison—a Samsung model that he wanted specifically because of its encryption capabilities. GX 821; GX 5003; Betances Tr. 2389. The following day, Schulte wrote in his notebook that "the way is clear. I will set up a word press . . . presumptionofinnocence.wordpress.com. From here, I will stage my information war." GX 809. In his notebooks, Schulte wrote about establishing various social media accounts that he would use to carry out this plan, and composed "to do lists" that included entries like "delete all google docs from john smith" and "delete all suspicious emails from my gmail." *Id.*

On August 22, 2018, Schulte (pretending to be another person) sent an email from an anonymous account to a reporter asking for copies of Schulte's articles. GX 1303-2. Schulte's notebook confirmed that it was Schulte who sent the August 22 email to the reporter, writing in an entry dated August 23, 2018, "Yesterday I started emailing [the reporter] from the Washington Post." GX 809. On September 1, 2018, he wrote draft tweets in his notebooks from the Twitter handle "@FreeJasonBourne," a fictional CIA operative, including: "The @ Dept of Justice arrested the wrong man for Vault 7. I personally know exactly what happened as do many others—why are they covering it up?"; the Bartender Tweet; and a tweet[5] directing others to "send all your govt's secrets here: Wikileaks." GX 809. In later entries in September, Schulte wrote that he planned to "Schedule tweets 27th" and "[i]n a week I'm going to dump all my stuff." *Id.*

On September 24, 2018, Schulte emailed the reporter from the anonymous email account attaching the search warrant subject to the protective order and his notes regarding Hickok[6]—a bridge between the DEVLAN system and another CIA network. GX 812. On October 3, 2018, the FBI searched MCC and seized the notebooks and contraband cellphone. Schlesinger Tr. 2471, 2644.

[5] The full draft reads:

> Your service, intense security investigations and pristine criminal history cant even get you bail. As Josh Schulte has said, you are denied a presumption of innocence. Ironic, you do your country's dirty work but when your country accuses you of a crime you are arrested & presumed guilty. Until your govt protects you and honors your service, send all your govt's secrets here: Wikileaks.

GX 809.

[6] Schulte's notes on Hickok appear in the context of trying to persuade the reporter that the FBI lied in their initial search warrant:

> [Statement from search warrant] 3 of 200 people in one CIA Group had access to classified info.
>
> [Schulte's response] In reality, two groups—EDG and COG and at least 400 people had access. They don't include COG who was connected to our DEVLAN through HICOC, an intermediary network that connected both COG and EDG → RECKLESS DISREGARD FOR THE TRUTH: There is absolutely NO reason they shouldn't have known this connection exists. Step one is narrowing down the possible suspects and to completely disregard an ENTIRE GROUP and HALF the suspects is reckless.

GX 812.

II. The Government's Late Disclosure & Defense Case

During trial, the night before the examination of CIA witness Michael, the Government informed defense counsel that the CIA had placed Michael on enforced administrative leave. When questioned by the Court, the Government revealed that the CIA decided to place Michael on leave the day he met with the AUSAs in this case and that the Government had known at the time in August 2019. *See* Tr. 1260–61. Michael's August 2019 meeting was not his first with the Government; he had met with the Government several times during the investigation into the Wikileaks disclosure, dating back to early 2017. *See e.g.*, Michael Tr. 1272–73. But at the August 16, 2019 meeting, Michael told the Government he did not believe Schulte had done the reversion on April 20, 2016. *Id.* at 1313. That same day, the CIA drafted a memorandum requesting that Michael be placed on enforced administrative leave. *See* DX L. By the time Michael returned to Virginia following his interview on Friday, August 16, 2019, he received a call from his division chief directing him to meet at the CIA on Monday at a different entrance. Michael Tr. 1318–19.

As the Court indicated during trial, the Government should have disclosed Michael's enforced leave, which the Government knew six months before trial, at or about the time that the decision was made and should not have withheld it until the witness took the stand. Tr. 1334. The Court ordered the Government to produce the memorandum drafted by the CIA's Counterintelligence Mission Center ("CIMC"), dated August 16, 2019, recommending that Michael be placed on enforced administrative leave (the "CIMC Memo"). Tr. 1262. The Court allowed defense counsel to suspend the examination of Michael with the option of recalling him later. Tr. 1332. The Court also allowed the defense to introduce the CIMC Memo into evidence. *See* DX L. Ultimately, the Court granted the defense's request for an adverse jury instruction, which, among other things, advised the jurors that the Government had only revealed Michael's enforced leave during trial and that it should have done so sooner. *See* Tr. 2943.

Schulte called one witness, paralegal Achal Fernando-Peiris, who read the CIMC Memo into evidence. DX L. The CIMC Memo was dated August 16, 2019, the same day Michael met with the AUSAs and FBI. *See id.* The memo described Michael as an "employee who is associated with the investigation into the theft and unauthorized disclosure of Center for Cyber Intelligence (CCI) classified information published by Wikileaks beginning in March 2017." *Id.* CIMC requested "enforced administrative leave" for Michael "until the investigation into his knowledge of the theft of the CCI cyber toolkit is resolved." *Id.*

The CIMC Memo indicated that Michael's "lack of cooperation with inquiries into his past activities with [Schulte]" and his "unexplained activities" on DEVLAN, the system from which the data was stolen, "raises significant concern about his truthfulness, trustworthiness, and willingness to cooperate." DX L. In its "Investigation" section, the memo continued: "In support of the ongoing criminal investigation, CIMC conducted comprehensive reviews of all individuals who could have perpetrated the theft of the CCI data, including Michael" and that "several concerns about Michael have emerged in the review, including his close proximity to the theft of the data and his relationship with Joshua Schulte, the individual charged with the theft of the data." *Id.* CIMC added that "[f]orensic analysis of [Michael's] activity on DevLAN suggests [Michael] may have additional knowledge of anomalies on the system at the time of theft." *Id.*

Finally, the CIMC Memo provided a "Risk Assessment" indicating that Michael had "failed to provide clear and verifiable information concerning his activities in the workplace around the time of the theft"; that Michael's "behavior suggests he has knowledge of details of the theft that he ha[d] not divulged"; and that CIMC viewed Michael's "lack of cooperation as a significant and untenable risk to the security of the operations on which he now works and any new tools he deploys for [the Center for Cyber Intelligence]." DX L.

III. The Government's Rebuttal Witness

The jury heard testimony from the Government's rebuttal witness, Carter Hall, who oversaw the drafting of the CIMC Memo. Hall testified that the CIA did not suspect Michael as being involved in the leaks. Hall Tr. 2684. In sum, Hall testified that CIMC's urgent request for enforced administrative leave in August 2019 was actually based on Michael's lack of cooperation during the investigation, including about (1) a physical altercation between Michael and Schulte that had happened more than three years earlier; (2) the altercation between Schulte and Amol in 2016; and (3) the screenshot that Michael had taken the day of the reversion in 2016. *Id.* at 2686–89, 2704.

IV. Procedural History

The operative indictment in this case charged Schulte with ten counts.[7] *See* Jury Charge, ECF No. 345. At the close of the Government's case and again after the Government's rebuttal witness, Schulte moved for a judgment of acquittal pursuant to Federal Rule of Criminal Procedure 29. The Court reserved ruling on Schulte's motion. On March 9, 2020, after a four-week trial and nearly a week of deliberations, a jury returned a partial verdict and convicted Schulte of two counts: making false statements to law enforcement and contempt of court. The jury failed to reach a verdict on the remaining eight counts, and, as a result, the Court granted a mistral as to those counts. On May 15, 2020, Schulte filed the instant motion renewing his Rule 29 motion.

[7] *See* S2, ECF No. 68. Several months after the first trial, Schulte was reindicted, and currently awaits a second trial whose date has yet to be set. *See* S3, ECF No. 405.

DISCUSSION

Schulte moves for acquittal as to all counts, including the eight counts on which the jury failed to reach a verdict. Schulte's filing itself, however, focuses only on the count charging Schulte with theft of Government property, in violation of 18 U.S.C. § 641.[8] Schulte relegates to a footnote the argument that the Government presented insufficient evidence as a matter of law as to all counts. *See* Def. Mot. at 1 n.1. This approach—while unhelpful to the Court in resolving this motion—is permissible; specificity is not required under Rule 29. *See United States v. Gjurashaj*, 706 F.2d 395, 399 (2d Cir. 1983) ("[W]hen a defendant moves for acquittal, even without specificity as to the grounds, it is incumbent upon the government to review its proof as to the facts required to establish each element of each offense alleged.").[9]

I. Rule 29 Standard

To grant a motion for acquittal under Rule 29, a court must find that the evidence was legally insufficient to establish the defendant's guilt beyond a reasonable doubt. *See* Fed. R. Crim. P. 29; *Smith v. Massachusetts*, 543 U.S. 462, 468 (2005) ("[T]he Rule 29 judgment of acquittal is a substantive determination that the prosecution has failed to carry its burden."). Under Rule 29(c)(2), a court may enter a judgment of acquittal either where the jury has returned a guilty verdict or where the jury has failed to return a verdict. Fed. R. Crim. P. 29(c)(2); *see also United States v. Martin Linen Supply Co.*, 430 U.S. 564, 575 (1977) ("To the extent the judge's authority under Rule 29 is designed to provide additional protection to a defendant by filtering out deficient prosecutions, the defendant's interest in such protection is essentially identical both before the jury

[8] Schulte's motion notes that it focuses on the theft of Government property "without waiving its general motion for acquittal." Def. Mot. at 1.

[9] In this respect, the Criminal Rules differ from the Civil Rules. Rule 50(a)(2) of the Federal Rules of Civil Procedure requires that a motion for a directed verdict in a civil action shall state the specific grounds therefor. Rule 29 contains no such language. *See* Fed. R. Crim. P. 29.

is allowed to come to a verdict and after the jury is unable to reach a verdict . . . .").

When considering a Rule 29 motion, "[t]he Court must view the evidence in a light that is most favorable to the government, and with all reasonable inferences resolved in favor of the government." *United States v. Anderson*, 747 F.3d 51, 60 (2d Cir. 2014) (internal citations omitted). "The question is not whether this Court believes that the evidence at trial established guilt beyond a reasonable doubt, but rather, whether *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Mi Sun Cho*, 713 F.3d 716, 720 (2d Cir. 2013) (per curiam) (internal citations omitted). In a close case, where "either of the two results, a reasonable doubt or no reasonable doubt, is fairly possible, the court must let the jury decide the matter." *United States v. Autuori*, 212 F.3d 105, 114 (2d Cir. 2000) (internal citations omitted).

In assessing a sufficiency challenge, the Court reviews the evidence "in its totality, not in isolation." *Anderson*, 747 F.3d at 59. Direct evidence is not required; the Government is entitled to prove its case solely through circumstantial evidence and it need not negate every theory of innocence. *Glenn*, 312 F.3d at 63. Where a fact to be proved is also an element of the offense, however, "it is not enough that the inferences in the government's favor are permissible." *United States v. Martinez,* 54 F.3d 1040, 1043 (2d Cir. 1995). A court "must also be satisfied that the inferences are sufficiently supported to permit a rational juror to find that the element, like all elements, is established beyond a reasonable doubt." *Id.* "[I]f the evidence viewed in the light most favorable to the prosecution gives 'equal or nearly equal circumstantial support to a theory of guilt and a theory of innocence,' then 'a reasonable jury must necessarily entertain a reasonable doubt.'" *Glenn,* 312 F.3d at 70.

II. Application

The Court notes at the outset that Schulte's motion with respect to the federal larceny count (Count Five), 18 U.S.C. § 641, is moot because the Government has dismissed the count post-trial.[10] *See United States v. Schulte*, 17-CR-548 (PAC), Minute Entry (S.D.N.Y. July 1, 2020).

A. Counts One, Two, and Three: Theft, Transmission, and Attempted Transmission of National Defense Information

The Court now turns to the heart of this case. Counts One, Two, and Three charged Schulte with the theft and transmission of national defense information, in violation of 18 U.S.C. §§ 793(b) and (e). The two provisions proscribe different acts: § 793(b) (Count One) criminalizes unlawfully taking documents, notes or other items connected with the national defense for the purpose of obtaining national defense information with the intent or reason to believe it would be used to harm the United States; § 793(e) (Counts Two and Three) penalizes, *inter alia*, the unlawful transmission of national defense information with reason to believe the transmission could harm the United States. Counts One and Two arise from Schulte's conduct while at the CIA. Count Three's charged conduct occurred while Schulte was incarcerated at MCC.

To prove Count One, under § 793(b), the Government had to satisfy the following elements: (i) that Schulte copied, took, or obtained a document, note, or information; (ii) that the information was connected to the national defense; and (iii) that Schulte acted with the purpose of obtaining information respecting the national defense and with the intent or reason to believe the information was to be used to the injury of the United States. *See* Jury Charge at 23. To prove Counts Two and Three, under § 793(e), the Government was required to demonstrate that: (i)

[10] Count Six of the Second Superseding Indictment (*see* S2), theft of government property as proscribed under 18 U.S.C. § 641, was renumbered for the jury as Count Five. *See* Jury Charge at 38.

Schulte had unauthorized possession of, access to, or control over the document or information in question; (ii) the document or information in question was related to the national defense; (iii) Schulte had reason to believe that the document or information could be used to the injury of the United States; and (iv) Schulte willfully communicated (or delivered or transmitted or caused to be communicated, delivered, or transmitted) or attempted to transmit the document or information to a person who was not entitled to receive it. *See id.* at 26, 29.

1. National Defense Information

There is no dispute that the evidence presented at trial established that the information charged in Counts One and Two (i.e., the Alta Backup Files) constituted national defense information. National defense information is a broad, inclusive term "referring to the military and naval establishments and the related activities of national preparedness." *Gorin v. United States*, 312 U.S. 19, 28 (1941) (internal citations omitted). To qualify as national defense information, the materials or information in question must also be closely held by the United States. *See United States v. Heine,* 151 F.2d 813, 815–17 (2d Cir. 1945) (L. Hand, J.). Evidence presented at trial convincingly established that the Alta Backup Files contained the CIA's work product concerning classified cyber tools used to collect intelligence from foreign actors and the underlying source code for those tools; the Government also demonstrated how discovery of CIA tradecraft jeopardized the use and implementation of those tools. Further, the information was stored on a CIA system (DEVLAN) that was classified as top secret (*see* Weber Tr., 168–70; Leonis Tr. 552–53)—which, although not dispositive, tends to show that the information was closely held. *See United States v. Abu-Jihaad*, 630 F.3d 102, 135 (2d Cir. 2010); *United States v. Soblen*, 301 F.2d 236, 239 n. 2 (2d Cir. 1962). This evidence was sufficient for a jury to conclude beyond a reasonable doubt that the information was connected to the national defense.

The information charged in Count Three (the "MCC Leaked Information") presents more difficulty. The MCC Leaked Information includes: (1) the draft tweet about the classified cyber tool, Bartender, (2) Schulte's "Malware of the Mind" article describing techniques his group at the CIA used to hide data, and (3) the "Hickok Disclosure" revealing that DEVLAN was connected to another CIA computer network.

With respect to the Bartender tweet and "Malware of the Mind," the Court concludes the evidence was sufficient to reach the jury. During trial, jurors heard testimony that the disclosure of CIA tradecraft information disrupts the CIA's development and deployment of cyber tools that may be used against foreign actors, hindering intelligence gathering and making it easier for adversaries to detect the CIA on its system. *See Solben*, 301 F.2d at 239 n.2 (jurors instructed to consider "the alleged source, origin, character and utility of the information and documents" when evaluating purported national defense information). The Government also presented evidence demonstrating that the information was closely held, including that it was classified and was stored on a classified system. *See Abu-Jihaad*, 630 F.3d at 135.

The Court, however, concludes that the evidence presented at trial was insufficient to establish beyond a reasonable doubt that the Hickok information (i.e., that Hickok connected DEVLAN to another group's network) was national defense information. The Government elicited no testimony establishing how this information related to national defense or explaining the utility of such information. *See* GX 616 (Hickok User Guide marked unclassified).[11]

[11] Nor was there any evidence showing Schulte had reason to believe that the Hickok disclosure could harm the United States. At trial, the Government offered only vague testimony that if someone learned of Hickok "it could be used for other folks to subvert a system, to move information between two networks that does not need to get moved." Dave Tr. 786–87. There was no explanation of how Schulte's September 2018 disclosure, of DEVLAN's bridge to another group's network, could be used to the injury of the United States when the CIA had ceased using DEVLAN over a year earlier on March 7, 2017. *See* Weber Tr. 249–50.

2. Disclosure and Transmission by Schulte

The central question of fact at trial concerned whether the evidence presented was sufficient to prove that Schulte was the source of CIA cyber tool information released by Wikileaks in 2017. The Court notes at the outset that the evidence presented at trial gives rise to competing inferences. Importantly, because access to, taking of, and transmission of the information are all—in addition to "fact[s] to be proved"—essential elements of the charged offenses, "it is not enough that the inferences in the government's favor are *permissible*." *Martinez*, 54 F.3d at 1043 (emphasis added). Rather, those elemental facts must, "like all elements, [be] established beyond a reasonable doubt." *Id.*

Access and Copying. To establish that Schulte illegally accessed and took the information on April 20, 2016, the Government presented evidence showing that (1) Schulte had a motive to disclose classified CIA information, arising from management's decisions in the aftermath of his tiff with Amol (*see* Tr. 2853); (2) Schulte reverted DEVLAN to a state where he had full administrative privileges and thus, had the opportunity to access the stolen files; (3) the stolen Confluence Alta Backup File date-accessed timestamp was modified during the reversion; (4) the system was reverted for a long enough time to copy the stolen files; (5) Schulte deleted log files on the OSB Server that would have shown his activity on the system; and (6) Schulte was, in fact, at his DEVLAN computer during the reversion. The Government further presented testimony that there was no legitimate reason for Schulte to have reverted the system or to delete the log files and April 20 snapshot. Finally, the Government also spotlighted Schulte's irregular post-reversion activity on his home computer.

Schulte's defenses were not insubstantial. They included: (1) DEVLAN's significant security shortcomings; (2) the fact that CIA employees knew DEVLAN was vulnerable; (3) that the Government had no evidence demonstrating precisely how Schulte transferred the information from an air-gapped, classified system to his home; (4) that Schulte's group's mission was to hack foreign actors precisely in this manner and thus, many others had a motive to exploit DEVLAN; and (5) that Michael—who was present when the CIA information was stolen, took a screenshot of the reversion that he never disclosed until 2017, and was later placed on enforced leave by the CIA in connection with the investigation—was also a suspect.

The defense sought to undermine the inference that Schulte stole the Alta Backup Files by demonstrating DEVLAN's insecurity. Their competing inference was, in effect, that because DEVLAN was so insecure, many more people had access and opportunity to commit the theft than the Government's immediate focus on Schulte would suggest. This uncertainty, per the defense, was only magnified by the CIA's decision to place Michael on enforced leave in August 2019—and to not disclose this fact until the middle of trial.

Nonetheless, the Court concludes, viewing the evidence in the light most favorable to the Government, that the Government presented sufficient evidence to permit a juror to conclude that Schulte copied and had unlawful access to, or control over, the stolen Alta Backup Files. Evidence at trial persuasively established that these files were accessed during the reversion, that there was no legitimate reason under the circumstances to revert the system, and that the log files and the snapshot were deleted. The inference that Schulte copied the information is bolstered by his irregular activity on his home computer the following week, including, *inter alia*, his downloading of Tails, mounting of his encrypted container, the frequent overnight check-ins, and his searches related to hashing and confirming that 1TB of data transferred correctly. *See Glenn*, 312 F.3d at 63 (explaining that the Court views the evidence in its totality, not in isolation and that the Government need not negate every theory of innocence). While the Court again acknowledges that there are competing inferences, it is the *jury's* role to choose among such inferences where, as here, the evidence is sufficient. *See United States v. Burden,* 600 F.3d 204, 214 (2d Cir. 2010).

Transmission. To prove transmission of the Alta Backup Files, an essential element of § 793(e) (Count Two), the Government relied on circumstantial evidence including: (1) Schulte's system reversion, corresponding with the time the Alta Backup File was accessed on April 20, 2016; (2) Schulte downloading, on his home computer, programs facilitating the anonymous and secure transfer of data, including programs recommended by Wikileaks; (3) Schulte's purchase of external hard drives for same-day delivery; (4) Schulte's Google searches regarding "wiping" or deleting data, searches regarding "hashing" a technique used when transferring data, as well as searches regarding transferring 1TB of data; (5) Schulte's actions on his computer during and throughout the middle of the night on April 30 to May 1, 2016; (6) Schulte's complete reformatting of his computer on May 5, 2016, which had the effect of erasing data; and (7) Schulte's increased interest in Wikileaks in the summer and fall of 2016. The jury also heard testimony that it would have taken Wikileaks a significant time to reconstruct the leaked data sent because of an error in the Alta Backup script, explaining the delay between theft and publication embedded in the Government's theory of the case.

In response, the defense argued (1) that the timing of the Wikileaks disclosure, which occurred nearly a year after the alleged transmission, did not make sense; and (2) that Schulte was not the average computer user and thus, many of the purportedly suspect actions were routine for him, including secure deletions, using anonymous browsers (e.g., TOR), and purchases of external hard drives. The defense also established that Schulte hosted (and was known by CIA employees to host) a significant movie collection. Berger Tr. 1423.

The Court concludes, viewing the evidence in the light most favorable to the Government, that a rational juror could find Schulte transmitted the Alta Backup Files to someone not entitled to receive it. The Government is permitted to rely solely on circumstantial evidence to establish transmission, including Schulte's motive, access to the Alta Backups, deletion of the log files and snapshot on April 20, 2016, irregular home computer activity following the reversion, and searches for technical information regarding transmitting data, as well as evidence that he wiped his computer and showed a marked increased interest in Wikileaks. *See United States v. Sureff*, 15 F.3d 225, 229 (2d Cir. 1994); *see also Abu-Jihaad*, 630 F.3d at 135–39 (holding circumstantial evidence of defendant's access to information, motive to transmit the information, prior contact with the recipient of the information, previous disclosure of classified information, and attempts to destroy evidence sufficient to support conviction for transmission of information). While any given juror, of course, may find the defense's inferences more persuasive than the Government's, it remains the province of the jury, not the Court, to choose among competing inferences supported by sufficient evidence. *See Autuori*, 212 F.3d at 114.

Count Three. To prove attempted unlawful possession of the MCC Leaked Information, the Government introduced Schulte's notebook, and the classified information contained therein. There is no dispute that Schulte was not authorized to possess classified information at MCC. Thus, a rational juror could find unlawful possession. *See United States v. Sterling*, 860 F.3d 233, 242 (4th Cir. 2017) (keeping classified information at defendant's home sufficient to support conviction under § 793, which requires the defendant to have "unauthorized possession" of the information).

The Government's evidence of attempted transmission of the MCC Leaked Information included evidence demonstrating that Schulte (1) wrote in his prison notebook about engaging in an "information war" and "desire to break up diplomatic relationships" (GX 809); (2) created social media accounts; (3) drafted tweets about a classified CIA cyber tool, Bartender; (4) drafted and attempted to publish an article entitled "Malware of the Mind" containing information about CIA tradecraft; (5) obtained and used a cellphone to access these social media and email accounts; and (6) tried to conceal his use of social media accounts and his efforts to publish the information including by using family and friends and deleting "suspicious emails from my gmail" (GX 809). Viewed in the light most favorable to the Government, the Court holds that a rational juror could conclude from this evidence that Schulte attempted to transmit national defense information with an intent to do something the law forbids. *See United States v. Desposito*, 704 F.3d 221, 233 (2d Cir. 2013) ("[A] rational jury could find beyond a reasonable doubt that his persistent writing and mailing of letters constituted substantial steps toward obstructing his criminal trial."); *United States v. Steele*, 390 F. App'x. 6, 12 n. 2 (2d Cir. 2010) ("[A]ssumption of a false name, and related conduct, are admissible as evidence of consciousness of guilt, and thus of guilt itself.") (internal citations omitted).

3. Harm to the United States

There is no dispute that Schulte had reason to believe that transmission of the Alta Backup Files would be used to the injury of the United States, as charged in Count One. The Government introduced (1) testimony demonstrating the public harms to the United States that had resulted from prior WikiLeaks disclosures (*see* Rosenzweig Tr. 44–55); (2) electronic chats in which Schulte demonstrated his knowledge of prior leaks (*see* GX 1405-7; GX 1405-8), and his understanding of the Government's need to protect some information from disclosure for national security reasons (GX 1405-10); (3) Schulte's CIA security agreements in which he acknowledged that the unauthorized disclosure of classified information could compromise CIA activities and harm the United States (*see* GX 401–405); (4) testimony from multiple CIA witnesses about the harms associated with revealing cyber tools and tradecraft; and (5) Schulte's emails and recorded interviews expressing his frustration that CIA management had mistreated him, which ultimately resulted in ending his career in the intelligence community. A rational juror could conclude from this evidence that Schulte had reason to believe that transmission and attempted transmission of the Alta Backup Files and prison writings would harm the United States, as charged in Counts Two and Three.

B. Counts Four, Six, and Seven: Unauthorized Computer Access

The evidence underlying Counts One and Two also substantiates Counts Four and Six. Counts Four and Six charge violations of 18 U.S.C. §§ 1030(a)(1) and (a)(2)(B). Both statutes require the Government to prove that Schulte accessed a computer initially with authorization, but then exceeded that authority by accessing and obtaining the information in question. *See* Jury Charge at 34, 41. Count Four further requires that the obtained information was protected from unauthorized disclosure "for reasons of national defense or foreign relations," that the defendant had reason to believe the information could be used against the interests of the United States, and that the defendant willfully communicated or transmitted the protected information. *Id.* at 34. Count Six requires that the obtained information be from an agency of the United States. *Id.* at 41.

The same evidence presented in support of Counts One and Two establish the essential elements in Counts Four and Six. *See id.* Accordingly, viewing the evidence in the light most favorable to the Government, a rational juror could find the essential elements of both counts.

Count Seven charges a violation of § 1030(a)(5)(A), which proscribes the intentional transmission of, among other things, any "code or command" that causes "damage" without authorization to a "protected computer." *Id.* The statute defines damage as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030)(e)(8).

Viewing the evidence in the light most favorable to the Government, the Court finds that a rational juror, based upon the reversion and deleted logs and snapshot as discussed above, could conclude that the essential elements of Count Seven have been satisfied.

C. Counts Eight and Nine: False Statements and Obstruction of Justice

Count Eight charged Schulte with making material false statements to the FBI and the U.S. Attorney's Office in violation of 18 U.S.C. § 1001. The jury reached a guilty verdict on Count Eight. Count Nine charges Schulte with obstructing the investigation into the Leaked Information. The jury failed to reach a verdict on Count Nine.

For Count Eight, the Government was required to prove beyond a reasonable doubt that Schulte knowingly and willfully made a material false or fraudulent statement to a U.S. law enforcement agency about a matter within that agency's jurisdiction. *See United States v. Coplan*, 703 F.3d 46, 78 (2d Cir. 2012). A false statement is material under § 1001 if it either had "a natural tendency to influence, or [is] capable of influencing, the decision of the decisionmaking body to which it was addressed," or if it is "capable of distracting government investigators' attention away from a critical matter." *United States v. Adekanbi*, 675 F.3d 178, 182 (2d Cir. 2012) (internal citations omitted). The jury heard testimony that Schulte made misrepresentations to the FBI and U.S. Attorney's Office, the offices responsible for conducting criminal investigations. These included, *inter alia*, Schulte's statement that he never intentionally made DEVLAN more vulnerable to attack, even though he in fact manipulated the system on April 20, 2016 and deleted related files. *See* Evanchec Tr. 2235. The Government elicited testimony that the network activity on April 20, 2016 was central to the Government's investigation, given that it occurred on the same day that the stolen and leaked Alta Backup Files were accessed. *Id.* at 2200. Additionally, the jury heard testimony that Schulte told the FBI he had not kept a copy of his email to OIG, which contained classified information (GX 1616; Leonis Tr. 642–43), but that the FBI later recovered a copy of the email at Schulte's apartment in New York (*see* Evanchec Tr. 2179). From this evidence, a rational juror could conclude beyond a reasonable doubt that Schulte's misstatement was knowing and intentional, particularly given that Schulte kept several emails from the CIA about his dispute with CIA management at his apartment (*see* GX 1118; Evanchec Tr. 2205, 2253), which supported the Government's theory at trial that Schulte remained motivated to retaliate against the CIA for the way he was treated.

For Count Nine, the Government was required to prove (i) that there was a pending judicial proceeding, (ii) that Schulte knew about that proceeding, and (iii) that Schulte corruptly sought to impede that proceeding. *See* Jury Charge at 50. As to the first two elements, the Government introduced evidence establishing that during the FBI's initial interview of Schulte, an FBI agent delivered two grand jury subpoenas to Schulte calling for his testimony and production of his cellphone. Evanchec Tr. 2218. The Government established the third element—that Schulte corruptly sought to impede the proceeding—through the same evidence of Schulte's misrepresentations charged in Count Eight. Viewing the evidence in the light most favorable to the Government, the Court again holds that a rational juror could find the essential elements satisfied.

D. Count Ten: Contempt

Finally, Schulte cannot credibly challenge the sufficiency of Count Ten, contempt of court, in violation of 18 U.S.C. § 401(3). To prove contempt of court, the Government must prove that "(i) the court entered a reasonably specific order; (ii) defendant knew of that order; (iii) defendant violated that order; and (iv) his violation was willful." *United States v. Cutler*, 58 F.3d 825, 834 (2d Cir. 1995) (cleaned up). Here, the Protective Order was clear that materials designated under it "may be disclosed only by defense counsel" (i.e., not Schulte, who was not yet *pro se* at the time) to a delineated list of individuals which did not include reporters. GX 828. Schulte acknowledged he understood this restriction at the May 21, 2018 conference. GX 829. Nevertheless, on September 24, 2018, he emailed a copy of a search warrant affidavit stamped as subject to the Protective Order to a reporter to convince the reporter to write about his case. *See* GX 812. Thus, the evidence underlying Count Ten is sufficient to support the jury's verdict as to Count Ten.

CONCLUSION

For the reasons stated, the Court denies Schulte's Rule 29 motion, except as it pertains to the Hickok disclosure. The Clerk of the Court is directed to terminate the motion at ECF No. 397.

Dated: New York, New York
November 9, 2021

SO ORDERED

Paul A Crotty

HONORABLE PAUL A. CROTTY
United States District Judge